



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,916	11/25/2003	Ranjit S. Narjala	042390.P17490	9801
45209	7590	02/20/2008		
INTEL/BLAKELY 1279 OAKMEAD PARKWAY SUNNYVALE, CA 94085-4040			EXAMINER PATEL, JAY P	
			ART UNIT	PAPER NUMBER
			2619	
			MAIL DATE	DELIVERY MODE
			02/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/723,916

Applicant(s)

NARJALA ET AL.

Examiner

Jay P. Patel

Art Unit

2619

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 January 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7, 9-11 and 13-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7, 9-11 and 13-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This office action is in response to the RCE/amendment filed on 1/11/2008.
2. Claims 1-5, 7, 9-11 and 13-17 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-5, 7, 9-11 and 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee (US Patent 7047561 B1) in view of Inoue et al. (US Patent 6167513).

In regards to claim 1, Lee shows in figure 5 a packet processing method to using a firewall in association with real-time Internet applications. After layer 3 and layer 4 processing is carried out at step 515, at step 520 the packet is split into TCP and UDP data. The process of figure 5 is carried out according to the functions of the network layers in figure 2, where layers 7 through 3 implement packet filter policy (establishing a policy manager).

Subsequently in steps 550 and 555, packet filtering is applied (examining the packet via one or more filters in the policy manager). In further regards, figure 1 illustrates a schematic diagram of a computer network including a hybrid firewall 100 inclusive of packet filter 106 (the policy manager having a set of policies represented by

filters). The packet filter 106 examines packets at layer 3 and layer 4 to selectively control the flow of data to and from networks 110 and 120. Packet filter 106, will follow predetermined security rules that specify which types of packets to allow to pass and which types of packets to block (see column 4, lines 40-45) (a first filter to examine a type of packet).

Furthermore, packets are allowed or blocked based on layer 3 information such as destination IP address (see column 4, lines 46-50) (or a destination of the packet via a second filter).

Returning to figure 5, if at step 555, a packet is allowed to pass through; at subsequent steps 560 and 565, TCP and IP headers are respectively added.

At step 565, an IP header is added to outgoing packet (dynamically determining whether to apply a mobile IP to the packet).

In further regards to claim 1, Lee fails to teach neither the filtering policies being applied on a mobile node using a mobile IP protocol nor associating mobile IP to the packet if the packet does not match with any of the filtering. Inoue teaches the above-mentioned limitation in figure 3 where a mobile IP network is shown with gateways 4a-4c and a mobile node 2. Furthermore, since a mobile IP network exists, Inoue is also reads on transmitting a packet via a mobile node (see figure 36, arrow going from MN 2 to CH3). The gateways, carryout filtering according to prescribe security policies for the mobile node (see column 11, lines 19-23).

Furthermore, in figure 20 case 6, where the mobile node is in an external network (where being inside the home network reads on the filtering criteria) and a

correspondent host in the home network, mobile IP is applied (see column 30, lines 9-19) and the packet format used is from figure 4D.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue. The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claim 2, Lee shows in steps 565 an IP header added to a packet.

In regards to claim 3, Lee in combinations with Inoue teaches all the limitations of parent claims 1 and 2. Lee fails to show new source and destination addresses being added to an IP header. Inoue however shows in figure 7, an inner IP header being added with a new source and destination addresses.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue. The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claim 4, figure 1 illustrates a schematic diagram of a computer network including a hybrid firewall 100 inclusive of packet filter 106. The packet filter 106 examines packets at layer 3 and layer 4 to selectively control the flow of data to and from networks 110 and 120. Packet filter 106, will follow predetermined security rules

(criteria) that specify which types of packets to allow to pass and which types of packets to block (see column 4, lines 40-45) (filter to examine a type of packet).

In further regards to claim 4, Lee shows in step 520, the data being split into TCP and UDP data and in steps 550 and 560, UDP packet filtering policy is applied.

In regards to claim 5, Lee shows in step 520, the data being split into TCP and UDP data and in steps 550 and 560, UDP packet filtering policy is applied.

In regards to claim 7, Lee shows in figure 5 a packet processing method to using a firewall in association with real-time Internet applications. After layer 3 and layer 4 processing is carried out at step 515, at step 520 the packet is split into TCP and UDP data. The process of figure 5 is carried out according to the functions of the network layers in figure 2, where layers 7 through 3 implement packet filter policy (establishing a policy manager).

Subsequently in steps 550 and 555, packet filtering is applied (examining the packet via one or more filters in the policy manager). In further regards, figure 1 illustrates a schematic diagram of a computer network including a hybrid firewall 100 inclusive of packet filter 106 (the policy manager having a set of policies represented by filters). The packet filter 106 examines packets at layer 3 and layer 4 to selectively control the flow of data to and from networks 110 and 120. Packet filter 106, will follow predetermined security rules that specify which types of packets to allow to pass and which types of packets to block (see column 4, lines 40-45) (a first filter to examine a type of packet).

Furthermore, packets are allowed or blocked based on layer 3 information such as destination IP address (see column 4, lines 46-50) (or a destination of the packet via a second filter).

Returning to figure 5, if at step 555, a packet is allowed to pass through; at subsequent steps 560 and 565, TCP and IP headers are respectively added.

At step 565, an IP header is added to outgoing packet (dynamically determining whether to apply a mobile IP to the packet).

In further regards to claim 7, Lee fails to teach neither the filtering policies being applied on a mobile node using a mobile IP protocol nor associating mobile IP to the packet if the packet does not match with any of the filtering. Inoue teaches the above-mentioned limitation in figure 3 where a mobile IP network is shown with gateways 4a-4c and a mobile node 2. Furthermore, since a mobile IP network exists, Inoue is also reads on transmitting a packet via a mobile node (see figure 36, arrow going from MN 2 to CH3). The gateways, carryout filtering according to prescribe security policies for the mobile node (see column 11, lines 19-23).

Furthermore, in figure 20 case 6, where the mobile node is in an external network (where being inside the home network reads on the filtering criteria) and a correspondent host in the home network, mobile IP is applied (see column 30, lines 9-19) and the packet format used is from figure 4D.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue.

The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claim 9, Lee in combinations with Inoue teaches all the limitations of parent claim 7. Lee fails to show new source and destination addresses being added to an IP header. Inoue however shows in figure 7, an inner IP header being added with a new source and destination addresses.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue. The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claims 10 and 11, Lee shows in step 520, the data being split into TCP and UDP data and in steps 550 and 560, UDP packet filtering policy is applied and at step 570, packet is send out.

In regards to claim 13, Lee shows in figure 5 a packet processing method to using a firewall in association with real-time Internet applications. After layer 3 and layer 4 processing is carried out at step 515, at step 520 the packet is split into TCP and UDP data. The process of figure 5 is carried out according to the functions of the network layers in figure 2, where layers 7 through 3 implement packet filter policy (establishing a policy manager).

Subsequently in steps 550 and 555, packet filtering is applied (examining the packet via one or more filters in the policy manager). In further regards, figure 1 illustrates a schematic diagram of a computer network including a hybrid firewall 100 inclusive of packet filter 106 (the policy manager having a set of policies represented by filters). The packet filter 106 examines packets at layer 3 and layer 4 to selectively control the flow of data to and from networks 110 and 120. Packet filter 106, will follow predetermined security rules that specify which types of packets to allow to pass and which types of packets to block (see column 4, lines 40-45) (a first filter to examine a type of packet).

Furthermore, packets are allowed or blocked based on layer 3 information such as destination IP address (see column 4, lines 46-50) (or a destination of the packet via a second filter).

Returning to figure 5, if at step 555, a packet is allowed to pass through; at subsequent steps 560 and 565, TCP and IP headers are respectively added.

At step 565, an IP header is added to outgoing packet (dynamically determining whether to apply a mobile IP to the packet).

In further regards to claim 13, Lee fails to teach neither the filtering policies being applied on a mobile node using a mobile IP protocol nor associating mobile IP to the packet if the packet does not match with any of the filtering. Inoue teaches the above-mentioned limitation in figure 3 where a mobile IP network is shown with gateways 4a-4c and a mobile node 2. Furthermore, since a mobile IP network exists, Inoue is also reads on transmitting a packet via a mobile node (see figure 36, arrow going from MN 2

to CH3). The gateways, carryout filtering according to prescribe security policies for the mobile node (see column 11, lines 19-23).

Furthermore, in figure 20 case 6, where the mobile node is in an external network (where being inside the home network reads on the filtering criteria) and a correspondent host in the home network, mobile IP is applied (see column 30, lines 9-19) and the packet format used is from figure 4D.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue. The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claim 14, Lee shows in steps 565 an IP header added to a packet.

In regards to claim 15, Lee in combinations with Inoue teaches all the limitations of parent claims 13 and 14. Lee fails to show new source and destination addresses being added to an IP header. Inoue however shows in figure 7, an inner IP header being added with a new source and destination addresses.

Therefore, it would have been obvious to one skilled in the art at the time the invention was made to incorporate the firewall processing method taught by Lee into a security policy implement by the gateways in the mobile IP network disclosed by Inoue. The motivation to do so would be to provide security for real time applications that use mobile IP.

In regards to claim 16, figure 1 illustrates a schematic diagram of a computer network including a hybrid firewall 100 inclusive of packet filter 106. The packet filter 106 examines packets at layer 3 and layer 4 to selectively control the flow of data to and from networks 110 and 120. Packet filter 106, will follow predetermined security rules (criteria) that specify which types of packets to allow to pass and which types of packets to block (see column 4, lines 40-45) (filter to examine a type of packet).

In further regards to claim 16, Lee shows in step 520, the data being split into TCP and UDP data and in steps 550 and 560, UDP packet filtering policy is applied.

In regards to claim 17, Lee shows in step 520, the data being split into TCP and UDP data and in steps 550 and 560, UDP packet filtering policy is applied.

Response to Arguments

5. Applicant's arguments with respect to claims 1-5, 7, 9-11 and 13-17 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jay P. Patel whose telephone number is (571) 272-3086. The examiner can normally be reached on M-F 9:00 am - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:
10/723,916
Art Unit: 2619

Page 11

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JPP 2/15/08
Jay P. Patel
Examiner
Art Unit 2619

EDAN . ORGAD
SUPERVISORY PATENT EXAMINER

Edm Orgad